CHAPTER 15

inspect ctiqbe コマンド～ inspect xdmcp コマンド

inspect ctiqbe

CTIQBE プロトコル インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect ctiqbe** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

inspect ctiqbe

no inspect ctiqbe

デフォルト

デフォルトでは、このコマンドはディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは 7.0 で追加されました。既存の **fixup** コマンドが廃止され、代わりにこのコマンドが追加されました。

使用上のガイドライン

inspect ctiqbe コマンドは、NAT、PAT、および双方向 NAT をサポートしている CTIQBE プロトコル インスペクションをイネーブルにします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、セキュリティ アプライアンス を越えてコール セットアップを行えるようになります。

Telephony Application Programming Interface（TAPI）および Java Telephony Application Programming Interface（JTAPI）は、多数の Cisco VoIP アプリケーションで使用されます。Computer Telephony Interface Quick Buffer Encoding（CTIQBE）は、Cisco TAPI Service Provider（TSP）によって Cisco CallManager と通信するために使用されます。

CTIQBE アプリケーション インスペクションの使用時に適用される制限を次にまとめます。

- CTIQBE アプリケーション インスペクションでは、**alias** コマンドを使用したコンフィギュレーションはサポートしていません。
- CTIQBE コールのステートフル フェールオーバーはサポートされて*いません*。
- **debug ctiqbe** コマンドを使用すると、メッセージ送信が遅延することがあり、これによってリアルタイム環境のパフォーマンスに影響が出る可能性があります。このデバッグまたはログをイネーブルにし、セキュリティ アプライアンス を介して Cisco IP SoftPhone でコール セットアップを完了できない場合は、Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。
- CTIQBE アプリケーション インスペクションでは、複数の TCP パケットにフラグメント化された CTIQBE メッセージはサポートして*いません*。

次に、CTIQBE アプリケーション インスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が、セキュリティ アプライアンスのそれぞれ異なるインターフェイスに接続された別々の Cisco CallManager に登録されている場合、これら 2 つの電話機間のコールが失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT の使用時に Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録させるには、TCP ポート 2748 を PAT（インターフェイス）アドレスと**同じポート**にスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect ctiqbe** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect ctiqbe** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect ctiqbe** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、CTIQBE インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（2748）上の CTIQBE トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map ctiqbe-port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# exit
hostname(config)# policy-map ctiqbe_policy
hostname(config-pmap)# class ctiqbe-port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# exit
hostname(config)# service-policy ctiqbe_policy interface outside
```

すべてのインターフェイスに対して CTIQBE インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
show conn	さまざまな接続タイプの接続状態を表示します。

コマンド	説明
show ctiqbe	セキュリティ アプライアンスを通じて確立された CTIQBE セッションに関する情報を表示します。CTIQBE インスペクション エンジンによって割り当てられたメディア接続に関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect dcerpc

エンドポイントマッパー宛ての DCERPC トラフィックのインスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect dcerpc** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect dcerpc [*map_name*]

no inspect dceprc [*map_name*]

構文の説明

map_name	（任意）DCERPC マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

inspect dcerpc コマンドは、DCERPC プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

例

次の例は、DCERPC インスペクション ポリシー マップを定義し、DCERPC のピンホールのタイムアウトを設定する方法を示しています。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc_map

hostname(config)# service-policy global-policy global
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
timeout pinhole	DCERPC ピンホールのタイムアウトを設定して、グローバル システムのピンホール タイムアウトを上書きします。

inspect dns

DNS インスペクションをイネーブルにしたり（ディセーブルになっている場合）、DNS インスペクション パラメータを設定したりするには、クラス コンフィギュレーション モードで **inspect dns** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。DNS インスペクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

inspect dns [*map_name*]

no inspect dns [*map_name*]

構文の説明

map_name	（任意）DNS マップの名前。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。
7.2(1)	このコマンドは、DNS インスペクションの追加パラメータを設定できるように変更されました。

使用上のガイドライン

DNS ガードは、セキュリティ アプライアンスによって DNS 応答が転送されるとすぐに、DNS クエリーに関連付けられている DNS セッションを切断します。また、DNS ガードはメッセージ交換をモニタして、DNS 応答の ID が DNS クエリーの ID と必ず一致するようにします。

DNS インスペクションがイネーブルになっている場合（デフォルト）、セキュリティ アプライアンスは次の追加タスクを実行します。

- **alias**、**static**、および **nat** コマンドを使用して設定されているコンフィギュレーションに基づいて、DNS レコードを変換します（DNS リライト）。変換は、DNS 応答の A レコードにのみ適用されます。そのため、PTR レコードを必要とする逆ルックアップは、DNS リライトの影響を受けません。

（注） 個々の A レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。

- 最大 DNS メッセージ長を指定します（デフォルトは 512 バイト、最大長は 65535 バイト）。パケット長が設定されている最大長よりも小さいことを検証するために、必要に応じて再構築が実行されます。最大長を超えた場合、パケットはドロップされます。
- ドメイン名の長さを 255 バイトに制限し、ラベルの長さを 63 バイトに制限します。
- DNS メッセージに圧縮ポインタが出現した場合、ポインタが参照するドメイン名の整合性を確認します。
- 圧縮ポインタのループが終了するかどうかを確認します。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元/宛先 IP アドレス、送信元/宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つだけ作成されます。DNS ID は *app_id* で追跡され、各 app_id のアイドルタイマーは独立して実行されます。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内だけであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力した場合、新しい DNS セッションによってリセットされている DNS 接続のアイドル タイマーが表示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS リライトの機能

DNS インスペクションがイネーブルであるとき、DNS リライトは、任意のインターフェイスから送信された DNS メッセージの NAT を完全にサポートします。

内部のネットワーク上のクライアントが、外部インターフェイス上の DNS サーバから送信される内部アドレスの DNS 解決を要求した場合、DNS A レコードは正しく変換されます。DNS インスペクション エンジンがディセーブルである場合、A レコードは変換されません。

DNS リライトは、次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイスにある場合、*DNS 応答*のパブリック アドレス（ルーティング可能なアドレスまたは「マッピング」アドレス）をプライベート アドレス（「実際の」アドレス）に変換します。
- DNS クライアントがパブリック インターフェイスにある場合、プライベート アドレスをパブリック アドレスに変換します。

DNS インスペクションがイネーブルのままである間、**alias**、**static**、または **nat** コマンドを使用して DNS リライトを設定できます。これらのコマンドの構文および機能の詳細については、該当するコマンド ページを参照してください。

例

次に、DNS メッセージの最大長を設定する例を示します。

```
hostname(config)# policy-map type inspect dns dns-inspect
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 1024
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug dns	DNS のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect esmtp

SMTP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect esmtp** コマンドを使用します。クラス コンフィギュレーション モードは、ポリシー マップ コンフィギュレーション モードからアクセス可能です。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect esmtp [*map_name*]

no inspect esmtp [*map_name*]

構文の説明

map_name	（任意）ESMTP マップの名前。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ESMTP アプリケーション インスペクションを使用すると、セキュリティ アプライアンスを通過できる SMTP コマンドの種類を制限し、モニタ機能を追加することによって、SMTP ベースの攻撃からより強固に保護できます。

ESMTP は SMTP プロトコルの拡張機能であり、ほとんどの点で SMTP と類似しています。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション インスペクション処理は、SMTP アプリケーション インスペクションに似ており、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

inspect esmtp コマンドには、以前 **fixup smtp** コマンドで提供されていた機能が含まれており、さらに一部の拡張 SMTP コマンドに対するサポートも追加されています。拡張 SMTP アプリケーション インスペクションでは、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTLS、および VRFY を含む拡張 SMTP コマンドに対するサポートが追加されています。7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）に対するサポートとあわせて、セキュリティ アプライアンスでは合計で 15 個の SMTP コマンドがサポートされています。

ATRN、ONEX、VERB、CHUNKING などのその他の拡張 SMTP コマンドおよびプライベート拡張はサポートされていません。サポートされないコマンドは、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

inspect esmtp コマンドは、サーバ SMTP バナーの「2」、「0」、「0」以外の文字をアスタリスクに変更します。Carriage Return（CR; 復帰）、および Linefeed（LF; 改行）は無視されます。

SMTP インスペクションがイネーブルの場合、次のルールが遵守されていないと、インタラクティブ SMTP に使用されている Telnet セッションは有効なコマンドを待機し、ファイアウォール esmtp ステート マシンはセッションのための正しい状態を保持します。このルールとは、SMTP コマンドは 4 文字以上である必要がある、SMTP コマンドは復帰と改行で終了している必要がある、および SMTP コマンドは次の返信を発行する前に応答を待機する必要がある、というものです。

SMTP サーバは数値の応答コードと人が読めるオプションのストリングを使用してクライアント要求に応答します。SMTP アプリケーション インスペクションは、ユーザが使用できるコマンドとサーバが返送するメッセージを制御し、その数を減らします。SMTP インスペクションは、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。
- SMTP コマンド応答シーケンスをモニタします。
- 監査証跡の生成：メール アドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

SMTP インスペクションでは、次の異常な署名がないかどうか、コマンドと応答のシーケンスをモニタします。

- 切り捨てられたコマンド
- 不正なコマンド終端（<CR><LR> で終了していない）
- MAIL from コマンドまたは RCPT to コマンドに対するパラメータとして PIPE シグニチャが見つかった場合、セッションは閉じられます。ユーザが設定することはできません。
- SMTP サーバによる不意の移行
- 未知のコマンドに対しては、セキュリティ アプライアンスはパケット内のすべての文字を X に変更します。この場合、サーバはクライアントに対してエラー コードを生成します。パケット内が変更されるため、TCP チェックサムの再計算または調整が必要になります。
- TCP ストリーム編集
- コマンド パイプライン

例

次の例に示すように、SMTP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（25）上の SMTP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map smtp-port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# exit
hostname(config)# policy-map smtp_policy
hostname(config-pmap)# class smtp-port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# exit
hostname(config)# service-policy smtp_policy interface outside
```

すべてのインターフェイスに対して SMTP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug esmtp	SMTP のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	SMTP を含む各種接続タイプの接続状態を表示します。

inspect ftp

ポートを FTP インスペクション用に設定したり、拡張インスペクションをイネーブルにしたりするには、クラス コンフィギュレーション モードで **inspect ftp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

構文の説明

map_name	FTP マップの名前。
strict	（任意）FTP トラフィックの拡張インスペクションをイネーブルにして、RFC 標準への準拠を強制します。

注意　FTP を上位のポートに移動する場合には注意が必要です。たとえば、FTP ポートを 2021 に設定した場合、ポート 2021 に対して開始されるすべての接続で、データ ペイロードが FTP コマンドとして解釈されます。

デフォルト

セキュリティ アプライアンスは、デフォルトではポート 21 で FTP をリッスンします。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。*map_name* オプションが追加されました。

使用上のガイドライン

FTP アプリケーション インスペクションは、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックなセカンダリ データ接続を準備します。
- **ftp** コマンド応答シーケンスを追跡します。
- 監査証跡の生成
- 埋め込み IP アドレスの NAT を実行します。

（注）　バナーを除いて、**inspect ftp** では FTP コマンドまたは応答をセグメント化する FTP サーバはサポートしていません。

FTP アプリケーション インスペクションによって、FTP データ転送用にセカンダリ チャネルが用意されます。ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスト作成のイベントに応答してチャネルが割り当てられますが、事前のネゴシエーションが必要です。ポートは、PORT または PASV コマンドを使用してネゴシエートされます。

（注）　FTP コントロール接続のポートだけを指定し、データ接続のポートは指定しないでください。セキュリティ アプライアンスのステートフル インスペクション エンジンは、必要に応じてダイナミックにデータ接続を準備します。

（注）　**no inspect ftp** コマンドを使用して、FTP インスペクション エンジンをディセーブルにすると、発信ユーザはパッシブ モードだけで接続を開始でき、着信 FTP はすべてディセーブルになります。

strict オプションの使用方法

strict オプションを使用すると、Web ブラウザは FTP 要求で組み込みコマンドを送信できなくなります。個々の **ftp** コマンドは、新しいコマンドが許可される前に承認される必要があります。組み込みコマンドを送信する接続は、ドロップされます。**strict** オプションを使用すると、FTP サーバは 227 コマンドしか生成できなくなり、FTP クライアントは PORT コマンドしか生成できなくなります。227 コマンドと PORT コマンドが、エラー文字列に表示されないように確認されます。

すべてのインターフェイスに対してストリクト FTP アプリケーション インスペクションをイネーブルにするには、**interface** コマンドの代わりに **global** パラメータを使用します。

注意　**strict** オプションを使用すると、RFC 標準に準拠していない FTP クライアントは切断されることがあります。

strict オプションがイネーブルの場合、次の異常なアクティビティに関して、各 **ftp** コマンドと応答シーケンスが追跡されます。

- 切り捨てされたコマンド : PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかが確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド : **ftp** コマンドが、RFC で要求されているとおりに <CR><LF> 文字で終了しているかどうかがチェックされます。終了していない場合は、接続が閉じられます。
- RETR コマンドと STOR コマンドのサイズ : これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラー メッセージがロギングされ、接続が閉じられます。
- コマンド スプーフィング : PORT コマンドは、常にクライアントから送信されます。PORT コマンドがサーバから送信される場合、TCP 接続は拒否されます。
- 応答スプーフィング : PASV 応答コマンド（227）は、常にサーバから送信されます。PASV 応答コマンドがクライアントから送信される場合、TCP 接続は拒否されます。これにより、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2.」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集

- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうかが調べられます。1 ～ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- セキュリティ アプライアンスは、SYST コマンドに対する FTP サーバ応答を X の連続に置き換えることで、FTP クライアントがサーバのシステム タイプを取得できないようにします。このデフォルト動作を上書きするには、FTP マップ コンフィギュレーション モードで **no mask-syst-reply** コマンドを使用します。

（注） セキュリティ アプライアンスの通過を許可しない特定の FTP コマンドを識別するには、FTP マップを識別し **request-command deny** コマンドを使用します。詳細については、**ftp-map** および **request-command deny** コマンドのページを参照してください。

FTP ログ メッセージ

FTP アプリケーション インスペクションでは、次のログ メッセージが生成されます。

- 取得またはアップロードされたファイルごとに監査レコード 302002 が生成されます。
- **ftp** コマンドが RETR または STOR であるかどうかがチェックされ、取得コマンドおよび格納コマンドがログに記録されます。
- ユーザ名は、IP アドレスを提供するテーブルを検索することで取得されます。
- ユーザ名、送信元 IP アドレス、宛先 IP アドレス、NAT アドレス、およびファイル操作がログに記録されます。
- メモリ不足によってセカンダリ ダイナミック チャネルの準備に失敗した場合、監査レコード 201005 が生成されます。

NAT と連携することにより、FTP アプリケーション インスペクションでは、アプリケーション ペイロード内の IP アドレスが変換されます。これは、RFC 959 に詳細に記述されています。

例

ユーザ名とパスワードを送信する前に、すべての FTP ユーザに接続時バナーが表示されます。デフォルトでは、このバナーには、ハッカーがシステムの弱点を特定するのに役立つバージョン情報が含まれます。このバナーをマスクする方法を次に示します。

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
hostname(config-pmap-p)# exit
hostname(config-pmap)# exit
hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp
hostname(config-cmap)# exit
hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy ftp-policy interface inside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
mask-syst-reply	FTP サーバ応答をクライアントに対して非表示にします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
request-command deny	不許可にする FTP コマンドを指定します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect gtp

GTP インスペクションをイネーブルまたはディセーブルにしたり、GTP トラフィックまたはトンネルを制御するための GTP マップを定義したりするには、クラス コンフィギュレーション モードで **inspect gtp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

（注）　GTP インスペクションには、特別なライセンスが必要です。必要なライセンスがない状態でセキュリティ アプライアンスで **inspect gtp** コマンドを入力すると、セキュリティ アプライアンスによってエラー メッセージが表示されます。

構文の説明

map_name	（任意）GTP マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

GTP は GPRS のトンネリング プロトコルであり、ワイヤレス ネットワークを介したセキュアなアクセスの提供に役立ちます。GPRS は、既存の GSM ネットワークとの統合を目的としたデータ ネットワーク アーキテクチャです。企業ネットワークおよびインターネットに対する連続したパケットスイッチド データ サービスをモバイル加入者に提供します。GTP の概要については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の「Applying Application Layer Protocol Inspection」の章を参照してください。

GTP のパラメータの定義に使用する特定のマップを識別するには、**gtp-map** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードを開始して、特定のマップを定義するためのさまざまなコマンドを入力できるようになります。基準を満たさないメッセージに対して指定できるアクションは、**drop**、**rate-limit** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントを**ログに記録**するかどうかも指定できます。

GTP マップを定義した後、**inspect gtp** コマンドを使用してマップをイネーブルにします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、**inspect** コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

GTP の既知のポートは次のとおりです。

- 3386
- 2123

次の機能は 7.0 ではサポートされていません。

- NAT、PAT、外部 NAT、エイリアス、およびポリシー NAT
- 3386、2123、および 2152 以外のポート
- トンネル IP パケットとその内容の検証

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect gtp** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect gtp** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect gtp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次に、アクセス リストを使用して GTP トラフィックを識別し、GTP マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config)# match access-list gtp-acl
hostname(config)# gtp-map gtp-policy
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy interface outside
```

（注） この例では、デフォルト値で GTP インスペクションをイネーブルにします。デフォルト値を変更するには、**gtp-map** コマンドのページと、GTP マップ コンフィギュレーション モードで入力する各コマンドのコマンド ページを参照してください。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。

コマンド	説明
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show service-policy inspect gtp	**inspect gtp** ポリシーのステータスおよび統計情報を表示します。

inspect h323

H.323 アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect h323** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect h323 {**h225** | **ras**} [*map_name*]

no inspect h323 {**h225** | **ras**} [*map_name*]

構文の説明

h225	H.225 シグナリング インスペクションをイネーブルにします。
map_name	（任意）H.323 マップの名前。
ras	RAS インスペクションをイネーブルにします。

デフォルト

デフォルトのポート割り当ては次のとおりです。

- h323 h225 1720
- h323 ras 1718 ～ 1719

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect h323 コマンドは、Cisco CallManager や VocalTec Gatekeeper などの H.323 に準拠したアプリケーションに対するサポートを提供します。H.323 は International Telecommunication Union（ITU; 国際電気通信連合）で定義されている、LAN を介したマルチメディア会議用のプロトコル スイートです。セキュリティ アプライアンスは、One Call Signaling Channel 上の Multiple Calls の H.323 v3 機能など、バージョン 4 までの H.323 をサポートしています。

H.323 インスペクションをイネーブルにした場合、セキュリティ アプライアンス は、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、セキュリティ アプライアンス でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、セキュリティ アプライアンス では ASN.1 デコーダを使用して H.323 メッセージを復号化します。

- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

H.323 の動作

H.323 のプロトコル コレクションでは、あわせて最大 2 つの TCP 接続と 4 ～ 6 つの UDP 接続を使用できます。FastStart では 1 つの TCP 接続だけを使用し、RAS では登録、許可、およびステータス用に単一の UDP 接続を使用します。

H.323 クライアントは最初に、TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立し、Q.931 コール設定を要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.245 接続は、コール ネゴシエーションとメディア チャネル設定に使用されます。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 インスペクションは、Q.931 TCP 接続をモニタして、H.245 ポート番号を決定します。H.323 端末で FastStart を使用していない場合、セキュリティ アプライアンスは H.225 メッセージのインスペクションに基づいて H.245 接続をダイナミックに割り当てます。

（注）　RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 インスペクションは、H.245 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。Real-Time Transport Protocol（RTP）はネゴシエートされたポート番号を使用し、RTP Control Protocol（RTCP）はすぐ次の上位ポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 インスペクションでは、次のポートが使用されます。

- 1718：ゲートキーパー検出に使用される UDP ポート
- 1719：RAS およびゲートキーパー検出に使用される UDP ポート
- 1720：TCP 制御ポート

ゲートキーパーからの ACF メッセージがセキュリティ アプライアンスを通過する場合は、H.225 接続用のピンホールが開かれます。H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーが使用されると、セキュリティ アプライアンスは ACF メッセージのインスペクションに基づいて H.225 接続を開きます。セキュリティ アプライアンスで ACF メッセージを確認できない場合は、H.225 コール シグナリング用に既知の H.323 ポート 1720 のアクセス リストを開くことが必要になる場合があります。

セキュリティ アプライアンスは H.225 メッセージを検査した後、H.245 チャネルをダイナミックに割り当てて、同様にフィックスアップする H.245 チャネルに接続します。これは、セキュリティ アプライアンスを通過した H.245 メッセージはすべて、H.245 アプリケーション インスペクションを通過し、埋め込み IP アドレスの NAT が実行され、ネゴシエートされたメディア チャネルが開かれることを意味します。

H.323 ITU 規準では、メッセージ長を定義する TPKT ヘッダーが最初に送信されてから、H.225 と H.245 が信頼できる接続上を送信されることが要求されています。TPKT ヘッダーは必ずしも H.225/H.245 メッセージと同じ TCP パケットで送信される必要はないため、セキュリティ アプライアンスではメッセージを正しく処理およびデコードするために TPKT 長を保持しておく必要があります。セキュリティ アプライアンスは接続ごとにデータ構造を保持し、そのデータ構造に次に想定されるメッセージの TPKT 長が格納されます。

セキュリティ アプライアンスで任意の IP アドレスの NAT を実行する必要がある場合は、チェックサム、User-User Information Element（UUIE）長、および TPKT（H.225 メッセージの TCP パケットに含まれている場合）を変更する必要があります。TPKT が別の TCP パケットで送信される場合、セキュリティ アプライアンスはその TPKT のプロキシ ACK を実行し、H.245 メッセージに新しい長さの新しい TPKT を付加します。

（注） セキュリティ アプライアンスは、TPKT に対する ACK の代理処理では TCP オプションをサポートしていません。

パケットが H.323 インスペクションを通過する各 UDP 接続は、H.323 接続としてマークされ、**timeout** コマンドを使用して設定した H.323 タイムアウト値でタイムアウトします。

制限事項

H.323 アプリケーション インスペクションの使用に関して、次の既知の問題および制限があります。

- スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。
- H.323 アプリケーション インスペクションは、同一セキュリティ レベルのインターフェイス間の NAT ではサポートされていません。
- NetMeeting クライアントが H.323 ゲートキーパーに登録されているときに、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイにコールを発信しようとすると、接続は確立されるが音声が双方向で聞こえないという現象が確認されています。この問題は、セキュリティ アプライアンス の問題ではありません。
- ネットワーク スタティックを設定する場合、そのネットワーク スタティックがサードパーティのネットマスクおよびアドレスと同じであると、すべての発信 H.323 接続が失敗します。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect h323** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect h323** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect h323** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、H.323 インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（1720）上の H.323 トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map h323-port
hostname(config-cmap)# match port tcp eq 1720
hostname(config-cmap)# exit
hostname(config)# policy-map h323_policy
hostname(config-pmap)# class h323-port
hostname(config-pmap-c)# inspect h323
hostname(config-pmap-c)# exit
hostname(config)# service-policy h323_policy interface outside
```

すべてのインターフェイスに対して H.323 インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
show h225	セキュリティ アプライアンスで確立されている H.225 セッションの情報を表示します。
show h245	スロー スタートを使用しているエンドポイントによってセキュリティ アプライアンス間で確立された H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンス間で確立された H.323 RAS セッションの情報を表示します。
timeout {**h225** | **h323**}	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

inspect http

HTTP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect http** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect http [*map_name*]

no inspect http [*map_name*]

構文の説明

map_name	（任意）HTTP マップの名前。

デフォルト

HTTP のデフォルト ポートは 80 です。

拡張 HTTP インスペクションは、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect http コマンドは、HTTP トラフィックに関連付けられている可能性のある特定の攻撃およびその他の脅威を防ぎます。HTTP インスペクションは、次のようないくつかの機能を実行します。

- 拡張 HTTP インスペクション
- N2H2 または Websense を使用する URL のスクリーニング
- Java と ActiveX のフィルタリング

後の 2 つの機能は、**filter** コマンドとともに設定します。

拡張 HTTP インスペクションでは、HTTP メッセージが RFC 2616 に準拠していること、RFC で規定されている方式またはサポートされている拡張方式を使用していること、および他のさまざまな基準に適合していることを検証します。多くの場合、これらの基準と基準を満たしていない場合のシステムの応答を設定できます。基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などの異なるコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

HTTP メッセージに適用できる基準は、次のとおりです。

- 設定可能リストに挙げられている方式が含まれていない。

- 特定の転送エンコーディング方式またはアプリケーション タイプ。
- HTTP トランザクションが RFC 仕様に従っている。
- メッセージ本文のサイズが設定可能な限度内である。
- 要求メッセージおよび応答メッセージのヘッダー サイズが設定可能な限度内である。
- URI 長が設定可能な限度内である。
- メッセージ本文の content-type がヘッダーと一致している。
- 応答メッセージの content-type が要求メッセージの *accept-type* フィールドと一致している。
- メッセージの content-type が事前定義済みの内部リストに含まれている。
- メッセージが HTTP RFC 形式の基準を満たしている。
- 選択したサポート対象アプリケーションの有無。
- 選択したエンコーディング タイプの有無。

（注） 基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などの異なるコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

拡張 HTTP インスペクションをイネーブルにするには、**inspect http** *http-map* コマンドを入力します。このコマンドで HTTP トラフィックに適用されるルールは、特定の HTTP マップで定義します。この HTTP マップを設定するには、**http-map** コマンドおよび HTTP マップ コンフィギュレーション モード コマンドを入力します。

（注） HTTP マップで HTTP インスペクションをイネーブルにした場合は、リセットおよびログ アクションを伴う厳格な HTTP インスペクションがデフォルトでイネーブルになります。インスペクションの失敗に対して実行するアクションは変更できますが、HTTP マップがイネーブルになっているかぎり、厳格なインスペクションはディセーブルにできません。

例

次に、HTTP トラフィックを識別し、HTTP マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

この例では、セキュリティ アプライアンスは次のコンテンツを含むトラフィックを検出したときに、接続をリセットして Syslog エントリを作成します。

- 100 バイト未満または 2000 バイトを超えるメッセージ
- サポートされていないコンテンツ タイプ
- 100 バイトを超える HTTP ヘッダー
- 100 バイトを超える URI

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	HTTP アプリケーション インスペクションに関する詳細情報を表示します。
debug http-map	HTTP マップに関連付けられているトラフィックに関する詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

inspect icmp

ICMP インスペクション エンジンを設定するには、クラス コンフィギュレーション モードで **inspect icmp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。

inspect icmp

no inspect icmp

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ICMP インスペクション エンジンを使用すると、TCP や UDP トラフィックのように ICMP トラフィックを検査できます。ICMP インスペクション エンジンを使用しない場合は、ACL で ICMP によるセキュリティ アプライアンスの通過を禁止することを推奨します。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンにより、それぞれの要求に対して 1 つの応答しか返されなくなり、正確なシーケンス番号が設定されるようになります。

ICMP インスペクションがディセーブルの場合（デフォルト設定）、セキュリティの低いインターフェイスからセキュリティの高いインターフェイスへの ICMP エコー応答メッセージは、ICMP エコー要求への応答であっても拒否されます。

例

次の例に示すように、ICMP アプリケーション インスペクション エンジンをイネーブルにします。この例では、ICMP プロトコル ID（IPv4 の場合は 1、IPv6 の場合は 58）を使用して ICMP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。
policy-map	セキュリティ アクションを 1 つ以上のトラフィック クラスに関連付けるポリシーを定義します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect icmp error

ICMP エラー メッセージに対してアプリケーション インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect icmp error** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。

inspect icmp error

no inspect icmp error

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

スタティック /NAT コンフィギュレーションに基づいて、ICMP エラー メッセージを送信する中間ホップの xlate を作成するには、**inspect icmp error** コマンドを使用します。デフォルトでは、セキュリティ アプライアンスでは中間ホップの IP アドレスは表示されません。ただし、**inspect icmp error** コマンドを使用すると、中間ホップの IP アドレスが表示されるようになります。セキュリティ アプライアンスは、変換後の IP アドレスでパケットを上書きします。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスのソフトウェアでは、パス MTU ディスカバリまたはホップバイホップ ディスカバリに関する ICMP エラー メッセージの生成時に、出力インターフェイス アドレスを送信元アドレスとして使用します。**inspect icmp error** コマンドを使用して ICMP エラー メッセージのアプリケーション インスペクションをイネーブルにすると、NAT もまたこの送信元アドレスに単独で適用されます。

イネーブルになっている場合、ICMP エラー インスペクション エンジンによって次のように ICMP パケットが変更されます。

- IP ヘッダーで、NAT IP が Client IP（宛先アドレスおよび中間ホップ アドレス）に変更され、IP チェックサムが変更されます。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。
  - 元のパケットの NAT IP が Client IP に変更されます。
  - 元のパケットの NAT ポートが Client Port に変更されます。
  - 元のパケットの IP チェックサムを再計算する。

ICMP エラー インスペクションがイネーブルかどうかに関係なく、ICMP エラー メッセージが取得されると、ICMP ペイロードがスキャンされ、元のパケットから 5 つのタプル（送信元 IP、宛先 IP、送信元ポート、宛先ポート、および IP プロトコル）が取得されます。クライアントの元のアドレスを確認し、特定の 5 つのタプルに関連付けられている既存のセッションを検索するために、取得した 5 つのタプルを使用してルックアップが実行されます。セッションが見つからなかった場合、ICMP エラー メッセージはドロップされます。

例

次の例に示すように、ICMP エラー アプリケーション インスペクション エンジンをイネーブルにします。この例では、ICMP プロトコル ID（IPv4 の場合は 1、IPv6 の場合は 58）を使用して ICMP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp error
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP エラー インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
icmp	セキュリティ アプライアンス インターフェイスで終了する ICMP トラフィックのアクセス ルールを設定します。
inspect icmp	ICMP インスペクション エンジンをイネーブルまたはディセーブルにします。
policy-map	セキュリティ アクションを 1 つ以上のトラフィック クラスに関連付けるポリシーを定義します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect ils

ILS アプリケーション インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect ils** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect ils

no inspect ils

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ils コマンドは、LDAP を使用してディレクトリ情報を ILS サーバと交換する Microsoft NetMeeting、SiteServer、および Active Directory 製品に対する NAT のサポートを提供します。

セキュリティ アプライアンス は ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、Port Address Translation（PAT; ポート アドレス交換）はサポートされません。

LDAP サーバが外部にある場合、内部ピアが外部 LDAP サーバに登録された状態でローカルに通信できるように、検索応答に対して NAT を行うことを検討してください。このような検索応答では、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0（NAT なし）を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるためにインスペクション エンジンをオフにすることをお勧めします。

ILS サーバがセキュリティ アプライアンス境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバにアクセスするためのホールが必要となります。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は一定の間隔 TCP アクティビティがなければ切断されます。デフォルトでは、この間隔は 60 分です。この値は、**timeout** コマンドを使用して調整できます。

ILS/LDAP はクライアント/サーバ モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバに BIND PDU が送信されます。サーバから成功を示す BIND RESPONSE を受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ（ADD、DEL、SEARCH、MODIFY など）が交換される場合があります。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される、NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS インスペクションでは、次の操作が実行されます。

- BER 復号化機能を使用して LDAP REQUEST PDU/RESPONSE PDU を復号化する。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスが含まれる PDU を符号化する。
- 新しく符号化された PDU を元の TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号の増分を調整する。

ILS インスペクションには、次の制限事項があります。

- 参照要求および応答はサポートされない。
- 複数のディレクトリ内のユーザは統合されない。
- 1 人のユーザが複数のディレクトリで複数の ID を持つ場合、NAT はそのユーザを認識できない。

（注） H225 コール シグナリング トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP **timeout** コマンドで指定された間隔が経過すると、TCP 接続は切断されます。デフォルトで、この間隔は 60 分に設定されています。

例

次の例に示すように、ILS インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（389）上の ILS トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map ils-port
hostname(config-cmap)# match port tcp eq 389
hostname(config-cmap)# exit
hostname(config)# policy-map ils_policy
hostname(config-pmap)# class ils-port
hostname(config-pmap-c)# inspect ils
hostname(config-pmap-c)# exit
hostname(config)# service-policy ils_policy interface outside
```

すべてのインターフェイスに対して ILS インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug ils	ILS のデバッグ情報をイネーブルにします。

コマンド	説明
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect im

IM トラフィックのインスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect im** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect im *map_name*

no inspect im *map_name*

構文の説明

map_name	IM マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

inspect im コマンドは、IM プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

例

次の例は、IM インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname4 "darshant\@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\.0"
hostname(config)# regex gif_files ".*\.gif"
hostname(config)# regex exe_files ".*\.exe"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4
```

```
hostname(config)# class-map type inspect im match-any yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
match protocol	インスペクション クラス マップまたはインスペクション ポリシー マップで、特定の IM プロトコルを一致させます。

inspect ipsec-pass-thru

IPSec Pass Thru インスペクションをイネーブルにするには、クラス マップ コンフィギュレーション モードで **inspect ipsec-pass-thru** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect ipsec-pass-thru [*map_name*]

no inspect ipsec-pass-thru [*map_name*]

構文の説明

map_name	（任意）IPSec Pass Thru マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

inspect ipsec-pass-thru コマンドは、アプリケーション インスペクションをイネーブルまたはディセーブルにします。IPSec Pass Through アプリケーション インスペクションによって、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）トラフィックか AH（IP プロトコル 51）トラフィックまたはその両方の便利なトラバーサルが提供されます。このインスペクションは、冗長なアクセス リスト コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

インスペクションのパラメータの定義に使用する特定のマップを識別するには、IPSec Pass Through パラメータ マップを使用します。パラメータ コンフィギュレーションにアクセスするには、**policy-map type inspect** コマンドを使用します。このコンフィギュレーションで、ESP または AH トラフィックの制限を指定できます。パラメータ コンフィギュレーションでは、クライアントあたりの最大接続数と、アイドル タイムアウトを設定できます。

class-map、**policy-map**、および **service-policy** の各コマンドを使用してトラフィックのクラスを定義し、**inspect** コマンドをクラスに適用して、ポリシーを 1 つまたは複数のインターフェイスに適用します。定義したパラメータ マップは、**inspect IPSec-pass-thru** コマンドで使用されたときにイネーブルになります。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。

（注）　ASA 7.0 では、**inspect ipsec-pass-thru** コマンドは ESP トラフィックの通過のみ許可していました。最新バージョンで同じ動作を保持するために、**inspect ipsec-pass-thru** コマンドが引数なしで指定されている場合は、ESP を許可するデフォルト マップが作成され、付加されます。このマップは **show running-config all** コマンドの出力で確認できます。

例

次に、アクセス リストを使用して IKE トラフィックを識別し、IPSec Pass Thru パラメータ マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。
match protocol	インスペクション クラス マップまたはインスペクション ポリシー マップで、特定の IM プロトコルを一致させます。

inspect mgcp

MGCP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect mgcp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

構文の説明

map_name	（任意）MGCP マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

MGCP を使用するには、通常、2 つ以上の **inspect** コマンドを設定する必要があります。1 つはゲートウェイがコマンドを受信するポート用で、もう 1 つはコール エージェントがコマンドを受信するポート用です。一般的に、コール エージェントはゲートウェイのデフォルト MGCP ポート 2427 にコマンドを送信し、ゲートウェイはコール エージェントのデフォルト MGCP ポート 2727 にコマンドを送信します。

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部コール制御要素からメディア ゲートウェイを制御するために使用されます。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。

メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブル モデムやケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。

- ビジネス ゲートウェイ。従来のデジタル PBX（構内交換機）インターフェイスまたは統合 *soft PBX* インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。

（注） MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判定します。これによって、セキュリティ アプライアンス を通過するフローが確立され、MGCP エンドポイントをコール エージェントに登録できます。

1 つ以上のコール エージェントおよびゲートウェイの IP アドレスを設定するには、MGCP マップ コンフィギュレーション モードで **call-agent** および **gateway** コマンドを使用します。コマンド キューで一度に許可される MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect mgcp** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect mgcp** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect mgcp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次に、MGCP トラフィックを指定し、MGCP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する例を示します。この例では、デフォルト ポート（2427 および 2727）上の MGCP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# access-list mgcp_acl permit tcp any any eq 2427
hostname(config)# access-list mgcp_acl permit tcp any any eq 2727
hostname(config)# class-map mgcp_port
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# exit
hostname(config)# mgcp-map inbound_mgcp
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
hostname(config-pmap-c)# exit
```

```
hostname(config)# service-policy inbound_policy interface outside
```

このコンフィギュレーションでは、コール エージェント 10.10.11.5 および 10.10.11.6 でゲートウェイ 10.10.10.115 を制御し、コール エージェント 10.10.11.7 および 10.10.11.8 で、10.10.10.116 と 10.10.10.117 の両方のゲートウェイを制御できるようにします。キューに入れることができる MGCP コマンドの最大数は 150 です。

すべてのインターフェイスに対して MGCP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug mgcp	MGCP のデバッグ情報をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	セキュリティ アプライアンスを通じて確立された MGCP セッションに関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect mmp

MMP インスペクション エンジンを設定するには、クラス コンフィギュレーション モードで **inspect mmp** コマンドを使用します。

MMP インスペクションを削除するには、このコマンドの **no** 形式を使用します。

inspect mmp tls-proxy [*name*]

no inspect mmp tls-proxy [*name*]

構文の説明

name	TLS プロキシ インスタンス名を指定します。
tls-proxy	MMP インスペクションに対して TLS プロキシをイネーブルにします。MMP プロトコルではさらに TCP トランスポートも使用できますが、CUMA クライアントでは TLS トランスポートしかサポートしていません。そのため、MMP インスペクションをイネーブルにするには tls-proxy キーワードが必要です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

ASA には、CUMA Mobile Multiplexing Protocol（MMP）を検証するインスペクション エンジンが含まれています。MMP は、CUMA クライアントとサーバ間でデータ エンティティを送信するためのデータ トランスポート プロトコルです。ASA が CUMA クライアントとサーバの間に配置されており、MMP パケットのインスペクションが必要な場合は、**inspect mmp** コマンドを使用します。

MMP トラフィックは TLS 接続でしか転送できないため、MMP インスペクションは TLS プロキシとともにイネーブルにする必要があります。

例

次に、**inspect mmp** コマンドを使用して MMP トラフィックを検査する例を示します。

```
hostname(config)# class-map mmp
hostname(config-cmap)# match port tcp eq 5443
hostname(config-cmap)# exit
hostname(config)# policy-map mmp-policy
hostname(config-pmap)# class mmp
hostname(config-pmap-c)# inspect mmp tls-proxy myproxy
```

```
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy mmp-policy interface outside
```

関連コマンド

コマンド	説明
tls-proxy	TLS プロキシ インスタンスを設定します。
debug mmp	MMP 検査イベントを表示します。

inspect netbios

NetBIOS アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect netbios** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect netbios [*map_name*]

no inspect netbios [*map_name*]

構文の説明

map_name	（任意）NetBIOS マップの名前。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect netbios コマンドは、NetBIOS プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

例

次に、NetBIOS インスペクション ポリシー マップを定義する例を示します。

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect pptp

PPTP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect pptp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect pptp

no inspect pptp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Point-to-Point Tunneling Protocol（PPTP）は、PPP トラフィックをトンネリングするためのプロトコルです。PPTP セッションは、1 つの TCP チャネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、PPTP GRE トンネルのネゴシエートと管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション インスペクションは、イネーブルになると、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するために必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 で定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP 制御チャネル上で修正バージョンの GRE（RFC 2637）がネゴシエートされたときに、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行*されません*。

具体的には、セキュリティ アプライアンスは、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通知されたバージョンがバージョン 1 でない場合、TCP 制御チャネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続と xlate は、後続のセカンダリ GRE データ トラフィックを許可するために、必要に応じてダイナミックに割り当てられます。

PPTP インスペクション エンジンは、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャネルで修正バージョンの GRE（RFC 2637）がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

RFC 2637 で定義されているように、PPTP プロトコルは、主に、モデム バンク PPTP Access Concentrator（PAC; PPTP アクセス コンセントレータ）から開始されたヘッドエンド PPTP Network Server（PNS; PPTP ネットワーク サーバ）への PPP セッションのトンネリングに使用されます。このように使用された場合、PAC がリモート クライアントで PNS がサーバです。

ただし、Windows によって VPN で使用された場合、この関係は逆になります。PNS は、中央のネットワークにアクセスするためにヘッドエンド PAC への接続を開始するリモートのシングル ユーザ PC です。

例

次の例に示すように、PPTP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（1723）上の PPTP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map pptp-port
hostname(config-cmap)# match port tcp eq 1723
hostname(config-cmap)# exit
hostname(config)# policy-map pptp_policy
hostname(config-pmap)# class pptp-port
hostname(config-pmap-c)# inspect pptp
hostname(config-pmap-c)# exit
hostname(config)# service-policy pptp_policy interface outside
```

すべてのインターフェイスに対して PPTP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug pptp	PPTP のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect radius-accouting

RADIUS アカウンティング インスペクションをイネーブルまたはディセーブルにしたり、トラフィックまたはトンネルを制御するためのマップを定義したりするには、クラス コンフィギュレーション モードで **inspect radius-accounting** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

inspect radius-accounting [*map_name*]

no inspect radius-accounting [*map_name*]

構文の説明

map_name	（任意）RADIUS アカウンティング マップの名前。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS アカウンティングのパラメータの定義に使用する特定のマップを作成するには、**radius-accounting** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードを開始して、特定のマップを定義するためのさまざまなコマンドを入力できるようになります。基準を満たさないメッセージに対して指定できるアクションは、**send**、**host**、**validate-attribute**、**enable gprs**、および **timeout users** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのコマンドには、**parameter** モードからアクセスできます。

RADIUS アカウンティング マップを定義した後、**inspect gtp** コマンドを使用してマップをイネーブルにします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、**inspect** コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

（注）　**inspect radius-accounting** コマンドは、**class-map type management** コマンドとのみ使用できます。

例

次に、アクセス リストを使用して RADIUS アカウンティング トラフィックを識別し、RADIUS アカウンティング マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# policy-map type inspect radius-accountin ra
```

（注）　この例では、デフォルト値で RADIUS アカウンティング インスペクションをイネーブルにします。デフォルト値を変更するには、**parameters** コマンドのページと、RADIUS アカウンティング コンフィギュレーション モードで入力する各コマンドのコマンド ページを参照してください。

関連コマンド

コマンド	説明
parameters	セキュリティ アクションを適用するトラフィック クラスを定義します。
class-map type management	アクションを適用するセキュリティ アプライアンス宛てのレイヤ 3 またはレイヤ 4 管理トラフィックを識別します。
show service-policy および **clear service-policy**	サービス ポリシー設定の表示とクリアを行います。
debug inspect radius-accounting	RADIUS アカウンティング インスペクションをデバッグします。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect rsh

RSH アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect rsh** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect rsh

no inspect rsh

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

例

次の例に示すように、RSH インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（514）上の RSH トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map rsh-port
hostname(config-cmap)# match port tcp eq 514
hostname(config-cmap)# exit
hostname(config)# policy-map rsh_policy
hostname(config-pmap)# class rsh-port
hostname(config-pmap-c)# inspect rsh
hostname(config-pmap-c)# exit
hostname(config)# service-policy rsh_policy interface outside
```

すべてのインターフェイスに対して RSH インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect rtsp

RTSP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect rtsp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect rtsp [*map_name*]

no inspect rtsp [*map_name*]

構文の説明

map_name	（任意）RTSP マップの名前。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect rtsp コマンドを使用すると、セキュリティ アプライアンスで RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV の各接続で使用されます。

（注） Cisco IP/TV では、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。セキュリティ アプライアンスは、RFC 2326 に準拠して、TCP だけをサポートします。この TCP コントロール チャネルは、クライアントに設定されているトランスポート モードに応じて、オーディオ/ビデオ トラフィックの送信に使用されるデータ チャネルをネゴシエートするために使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

セキュリティ アプライアンスは、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合は、サーバは セキュリティ アプライアンスとの相対位置関係で外部に存在することになるため、サーバから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージが発信方向である場合、セキュリティ アプライアンス は、ダイナミック チャネルを開く必要はありません。

RFC 2326 では、クライアントとサーバのポートを SETUP 応答メッセージ内に含める必要があるとは規定していないため、セキュリティ アプライアンスで状態を保持し、SETUP メッセージに含まれているクライアント ポートを記憶しておく必要があります。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバは、サーバ ポートだけで応答します。

RealPlayer の使用方法

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。セキュリティ アプライアンスでは、サーバからクライアントまたはその逆の **access-list** コマンド ステートメントを追加します。RealPlayer の場合、[Options] > [Preferences] > [Transport] > [RTSP] [Settings] をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] チェックボックスおよび [Attempt to use TCP for all content] チェックボックスをオンにします。セキュリティ アプライアンスで、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] チェックボックスをオンにします。マルチキャストでの使用ができないライブ コンテンツについては、セキュリティ アプライアンスで、**inspect rtsp** *port* コマンド ステートメントを追加します。

制限事項

inspect rtsp コマンドに適用される制約事項は次のとおりです。

- セキュリティ アプライアンス は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- セキュリティ アプライアンス には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- Cisco IP/TV の場合、セキュリティ アプライアンスがメッセージの SDP 部分に対して実行する NAT の数は、Content Manager のプログラム リストの数に比例します（プログラム リストごとに少なくとも 6 個の埋め込み IP アドレスを設定できます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。
- HTTP を介して配信されるメディア ストリームは、RTSP アプリケーション インスペクションではサポートされません。これは、RTSP インスペクションが HTTP クローキング（HTTP でラップされた RTSP）をサポートしていないためです。

例

次の例に示すように、RTSP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（554 および 8554）上の RTSP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# access-list rtsp-acl permit tcp any any eq 554
hostname(config)# access-list rtsp-acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp-acl
hostname(config-cmap)# exit
hostname(config)# policy-map rtsp_policy
hostname(config-pmap)# class rtsp-traffic
```

```
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)# exit
hostname(config)# service-policy rtsp_policy interface outside
```

すべてのインターフェイスに対して RTSP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug rtsp	RTSP のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect sip

SIP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect sip** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

構文の説明

phone-proxy *proxy_name*	指定したインスペクション セッションの Phone Proxy をイネーブルにします。
sip_map	SIP ポリシー マップ名を指定します。
tls-proxy *proxy_name*	指定されたインスペクション セッションで TLS プロキシをイネーブルにします。キーワード tls-proxy をレイヤ 7 ポリシー マップ名として使用することはできません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

SIP のデフォルトのポート割り当ては 5060 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	**tls-proxy** キーワードが追加されました。
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SIP は、IETF で定義されているように、VoIP コールをイネーブルにします。SIP は SDP と連携して、コール シグナリングを行います。SDP はメディア ストリームの詳細を指定します。SIP を使用すると、セキュリティ アプライアンスですべての SIP Voice over IP（VoIP）ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP の定義は、次の RFC に記載されています。

- SIP：Session Initiation Protocol、RFC 2543
- SDP：Session Description Protocol、RFC 2327

セキュリティ アプライアンス経由の SIP コールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディ

アの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。SIP インスペクションは、それらの埋め込まれた IP アドレスに NAT を適用します。

（注）　リモート エンドポイントが、セキュリティ アプライアンスで保護されているネットワーク上の SIP プロキシに対して登録を試行すると、登録は非常に特殊な条件で失敗します。この条件とは、リモート エンドポイントに PAT が設定されていること、SIP レジストラ サーバが外部ネットワーク上にあること、およびエンドポイントによってプロキシ サーバに送信された REGISTER メッセージの contact フィールドにポートがないことです。

インスタント メッセージング

インスタント メッセージとは、ほぼリアルタイムにユーザ間でメッセージを転送することです。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol（SIP）Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後、任意の時点で着信する可能性があります。たとえば、2 人のユーザはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP インスペクション エンジンは、設定した SIP タイムアウト値に応じてタイムアウトするピンホールを開きます。この値は、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP インスペクション エンジンを通過する必要があります。

（注）　現在は、チャット機能のみがサポートされています。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

技術的詳細

SIP インスペクションは、SIP テキストベースのメッセージに対して NAT を実行し、メッセージの SDP 部分のコンテンツ長を再計算して、パケット長およびチェックサムを再計算します。また、エンドポイントが受信すべきアドレスまたはポートとして、SIP メッセージの SDP 部分に指定されたポートに対するメディア接続をダイナミックに開きます。

SIP インスペクションには、コールと送信元および宛先を識別する SIP ペイロードの CALL_ID、FROM、TO インデックスが含まれるデータベースがあります。このデータベースに格納されるのは、SDP メディア情報フィールドに格納されていたメディア アドレスおよびメディア ポートと、メディア タイプです。1 つのセッションに対して、複数のメディア アドレスとポートが存在することが可能です。RTP/RTCP 接続は、これらのメディア アドレスおよびポートを使用して、2 つのエンドポイント間で開かれます。

最初のコール設定（INVITE）メッセージでは、既知のポート 5060 を使用する必要があります。ただし、後続のメッセージではこのポート番号を使用しないこともあります。SIP インスペクション エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。この処理は、メッセージを SIP アプリケーションに到達させて、NAT を実行するために行われます。

コールが設定されると、SIP セッションは「一時的な」状態にあると見なされます。この状態は、宛先エンドポイントがリッスンしている RTP メディア アドレスとポートを示す Response メッセージが受信されるまで維持されます。1 分以内に応答メッセージを受信できなかった場合は、シグナリング接続が切断されます。

最後のハンドシェイクが行われると、コール状態はアクティブに移り、シグナリング接続は、BYE メッセージが受信されるまで維持されます。

内部エンドポイントが、外部エンドポイントに発呼した場合、メディア ホールが、外部インターフェイスに対して開き、内部エンドポイントから送信された INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに、RTP/RTCP UDP パケットが流れることが許可されます。内部インターフェイスへの非請求 RTP/RTCP UDP パケットは、セキュリティ アプライアンスのコンフィギュレーションで特別に許可されていない限りセキュリティ アプライアンスを通過しません。

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、これは設定可能なタイムアウトであり、時間間隔は変更することが可能です。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect sip** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect sip** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect sip** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SIP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（5060）上の SIP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map sip-port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# exit
hostname(config)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# exit
hostname(config)# service-policy sip_policy interface outside
```

すべてのインターフェイスに対して SIP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
show sip	セキュリティ アプライアンスを介して確立された SIP セッションに関する情報を表示します。
debug sip	SIP のデバッグ情報をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

inspect skinny

SCCP（Skinny）アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect skinny** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

no inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

構文の説明

phone-proxy *proxy_name*	指定したインスペクション セッションの Phone Proxy をイネーブルにします。
skinny_map	skinny ポリシー マップ名を指定します。
tls-proxy *proxy_name*	指定されたインスペクション セッションで TLS プロキシをイネーブルにします。キーワード tls-proxy をレイヤ 7 ポリシー マップ名として使用することはできません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
8.0(2)	キーワード **tls-proxy** が追加されました。
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Skinny（または Simple）Client Control Protocol（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。SCCP クライアントは、Cisco CallManager とともに使用することで、H.323 準拠の端末と相互運用できます。セキュリティ アプライアンスのアプリケーション層機能は、SCCP バージョン 3.3 を認識します。アプリケーション層ソフトウェアの機能で、SCCP シグナリング パケットの NAT を提供することにより、すべての SCCP シグナリングおよびメディア パケットがセキュリティ アプライアンスを通過できるようになります。

SCCP プロトコルには、2.4、3.0.4、3.1.1、3.2、3.3.2 の 5 つのバージョンがあります。セキュリティ アプライアンスでは、バージョン 3.3.2 までのすべてのバージョンをサポートしています。は、SCCP に対して PAT と NAT の両方のサポートを提供しています。IP 電話で使用するグローバル IP アドレスの数を制限している場合は、PAT が必要です。

Cisco CallManager と Cisco IP Phone 間の通常のトラフィックでは SCCP が使用され、特別なコンフィギュレーションがない限り SCCP インスペクションで処理されます。セキュリティ アプライアンスでは、セキュリティ アプライアンスで TFTP サーバの場所を Cisco IP Phone および他の DHCP クライアントに送信できるようにする、DHCP オプション 150 および 66 もサポートしています。詳細については、**dhcp-server** コマンドを参照してください。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べてセキュリティの高いインターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングは**スタティック**である必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。ID スタティック エントリを使用すると、よりセキュリティの高いインターフェイスに配置されている Cisco CallManager で Cisco IP Phone からの登録を受け付けられるようになります。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、アクセス リストを使用して UDP ポート 69 の保護された TFTP サーバに接続する必要があります。TFTP サーバにはスタティック エントリが必要ですが、これは「ID」スタティック エントリである必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager と比べてセキュリティの*高い*インターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにするために、アクセス リストやスタティック エントリは必要ありません。

制限事項

SCCP に対する現在のバージョンの PAT および NAT サポートに適用される制限は、次のとおりです。

- PAT は、**alias** コマンドを使用しているコンフィギュレーションでは動作しません。
- 外部 NAT および PAT はサポート **されません**。

（注） SCCP コールのステートフル フェールオーバーは、コール設定の最中のコールを除いて、サポートされるようになりました。

内部 Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスまたはポートに設定されている場合、セキュリティ アプライアンスでは、現在、TFTP 経由で転送されるファイル コンテンツに対する NAT または PAT をサポートしていないため、外部 Cisco IP Phone の登録は失敗します。セキュリティ アプライアンスでは TFTP メッセージの NAT をサポートしており、TFTP ファイルがセキュリティ アプライアンスを通過するためのピンホールを開きますが、電話機の登録時に TFTP を使用して転送される Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager IP アドレスおよびポートは、セキュリティ アプライアンスでは変換できません。

シグナリング メッセージのインスペクション

シグナリング メッセージのインスペクションでは、多くの場合、**inspect skinny** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect skinny** コマンドではトンネル デフォルト ゲートウェイ ルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect skinny** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイ ルートを設定しないようにしてください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SCCP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（2000）上の SCCP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map skinny-port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)# policy-map skinny_policy
hostname(config-pmap)# class skinny-port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy skinny_policy interface outside
```

すべてのインターフェイスに対して SCCP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug skinny	SCCP のデバッグ情報をイネーブルにします。
show skinny	セキュリティ アプライアンスを通じて確立された SCCP セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

inspect snmp

SNMP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect snmp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect snmp *map_name*

no inspect snmp *map_name*

構文の説明

map_name	SNMP マップ名です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SNMP マップで指定した設定を使用して SNMP インスペクションをイネーブルにするには、inspect snmp コマンドを使用します。SNMP マップは **snmp-map** コマンドを使用して作成します。SNMP トラフィックを特定のバージョンの SNMP に制限するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。

以前のバージョンの SNMP はセキュリティが低いため、SNMP トラフィックをバージョン 2 に制限するようにセキュリティ ポリシーで要求する場合があります。SNMP の特定のバージョンを拒否するには、**snmp-map** コマンドを使用して作成する SNMP マップで、**deny version** コマンドを使用します。SNMP マップを設定した後、**inspect snmp** コマンドを使用してマップをイネーブルにし、**service-policy** コマンドを使用して 1 つ以上のインターフェイスにこのマップを適用します。

例

次に、SNMP トラフィックを識別し、SNMP マップを定義して、ポリシーを定義し、SNMP インスペクションをイネーブルにして、外部インターフェイスにポリシーを適用する例を示します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
```

```
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

すべてのインターフェイスに対してストリクト snmp アプリケーション インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect sqlnet

Oracle SQL*Net アプリケーション インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect sqlnet** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sqlnet

no inspect sqlnet

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

デフォルトのポート割り当ては 1521 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SQL*Net プロトコルは、さまざまなパケット タイプで構成されています。セキュリティ アプライアンスはこれらのパケットを処理して、セキュリティ アプライアンス のどちらの側の Oracle アプリケーションにも一貫性のあるデータ ストリームが表示されるようにします。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、Structured Query Language（SQL; 構造化照会言語）の IANA ポート割り当てとは一致しません。SQL*Net インスペクションを一連のポート番号に適用するには、**class-map** コマンドを使用します。

（注） SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインスペクションをディセーブルにします。SQL*Net インスペクションがイネーブルになっていると、セキュリティ アプライアンスはプロキシとして機能し、クライアントのウィンドウ サイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。

セキュリティ アプライアンスは、すべてのアドレスの NAT を実行し、パケット内のすべての埋め込みポートを検索して、SQL*Net バージョン 1 用に開きます。

SQL*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の各 TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker）は、NAT 対象のアドレスがあるかどうかがスキャンされません。また、インスペクションがパケット内に埋め込まれたポートにダイナミック接続を開くこともありません。

SQL*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかスキャンされます。データ長がゼロの Redirect メッセージがセキュリティ アプライアンスを通過すると、後続の Data または Redirect メッセージの NAT が実行され、ポートがダイナミックに開かれることを想定するフラグが接続データ構造に設定されます。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net インスペクション エンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、Data）とすべてのパケットは、ポートおよびアドレスがあるかどうかスキャンされます。アドレスの NAT が実行され、ポート接続が開かれます。

例

次の例に示すように、SQL*Net インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（1521）上の SQL*Net トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map sqlnet-port
hostname(config-cmap)# match port tcp eq 1521
hostname(config-cmap)# exit
hostname(config)# policy-map sqlnet_policy
hostname(config-pmap)# class sqlnet-port
hostname(config-pmap-c)# inspect sqlnet
hostname(config-pmap-c)# exit
hostname(config)# service-policy sqlnet_policy interface outside
```

すべてのインターフェイスに対して SQL*Net インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug sqlnet	SQL*Net のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	SQL*net など、さまざまな接続タイプの接続状態を表示します。

inspect sunrpc

Sun RPC アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc

no inspect sunrpc

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Sun RPC アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、ポリシー マップ クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。このモードにアクセスするには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc コマンドは、Sun RPC プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはシステムの任意のポートで実行できます。クライアントがサーバ上の Sun RPC サービスにアクセスしようとする場合には、サービスが実行されているポートを検出する必要があります。これを行うには、既知のポート 111 でポートマッパー プロセスを照会します。

クライアントはサービスの Sun RPC プログラム番号を送信して、ポート番号を取得します。この時点より、クライアント プログラムは Sun RPC クエリーをその新しいポートに送信します。サーバから応答が送信されると、セキュリティ アプライアンスはこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

（注） Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

例

次の例に示すように、RPC インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（111）上の RPC トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map sunrpc-port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sunrpc-port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

すべてのインターフェイスに対して RPC インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
clear configure sunrpc_server	**sunrpc-server** コマンドを使用して実行されているコンフィギュレーションを削除します。
clear sunrpc-server active	Sun RPC アプリケーション インスペクションによって、NFS または NIS などの特定のサービス用に開けられているピンホールをクリアします。
show running-config sunrpc-server	Sun RPC サービス テーブル コンフィギュレーションの情報を表示します。
sunrpc-server	NFS または NIS などの Sun RPC サービス用に、タイムアウトを指定してピンホールを作成できるようにします。
show sunrpc-server active	Sun RPC サービス用に開けられているピンホールを表示します。

inspect tftp

TFTP アプリケーション インスペクションをディセーブルにしたり、ディセーブルになっている場合にイネーブルにしたりするには、クラス コンフィギュレーション モードで **inspect tftp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect tftp

no inspect tftp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

デフォルトのポート割り当ては 69 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RFC 1350 に規定されている Trivial File Transfer Protocol（TFTP）は、TFTP サーバとクライアント間でファイルを読み書きするための簡易プロトコルです。

セキュリティ アプライアンスは、TFTP トラフィックを検査し、必要に応じてダイナミックに接続と変換を作成し、TFTP クライアントとサーバの間のファイル転送を許可します。具体的には、インスペクション エンジンは TFTP Read Request（RRQ; 読み取り要求）、Write Request（WRQ; 書き込み要求）、およびエラー通知（ERROR）を検査します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバの間に存在できる不完全なセカンダリ チャネルは 1 つまでです。サーバからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

例

次の例に示すように、TFTP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（69）上の TFTP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map tftp-port
hostname(config-cmap)# match port udp eq 69
hostname(config-cmap)# exit
hostname(config)# policy-map tftp_policy
hostname(config-pmap)# class tftp-port
hostname(config-pmap-c)# inspect tftp
hostname(config-pmap-c)# exit
hostname(config)# service-policy tftp_policy interface outside
```

すべてのインターフェイスに対して TFTP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect waas

WAAS アプリケーション インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで **inspect waas** コマンドを使用します。クラス コンフィギュレーション モードは、ポリシー マップ コンフィギュレーション モードからアクセス可能です。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect waas

no inspect waas

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、WAAS アプリケーション インスペクションをイネーブルにする方法を示します。

```
hostname(config-pmap-c)# inspect waas
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect xdmcp

XDMCP アプリケーション インスペクションをイネーブルにしたり、セキュリティ アプライアンスがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect xdmcp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

inspect xdmcp

no inspect xdmcp

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect xdmcp コマンドは、XDMCP プロトコルに対するアプリケーション インスペクションをイネーブルまたはディセーブルにします。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、セキュリティ アプライアンスは、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、セキュリティ アプライアンスで **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきかどうかが確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、セキュリティ アプライアンスが必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。

例

次の例に示すように、XDMCP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（177）上の XDMCP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
hostname(config)# class-map xdmcp-port
hostname(config-cmap)# match port tcp eq 177
hostname(config-cmap)# exit
hostname(config)# policy-map xdmcp_policy
hostname(config-pmap)# class xdmcp-port
hostname(config-pmap-c)# inspect xdmcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy xdmcp_policy interface outside
```

すべてのインターフェイスに対して XDMCP インスペクションをイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug xdmcp	XDMCP のデバッグ情報をイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。